PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Siani Lynne PEARSON et al.**	Examiner:	Matthew E HENEGHAN
Serial No.:	**10/088,258**	Art Unit:	2134
Filed:	March 13, 2002	Our Ref:	B-4528PCT 619575-6 30990134-3 US
For:	"TRUSTED PLATFORM FOR RESTRICTING USE OF DATA"	Date:	April 25, 2008
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Commissioner for Patents

Sir:

This is an appeal from the rejection dated November 26, 2007, for the above identified patent application. This Appeal Brief is being timely filed in support of the Notice of Appeal filed on February 26, 2008. Please deduct the amount of $510.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief from deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 3, 6-10, 15-17, and 19-30 are pending in this application, stand rejected, are the subject of this Appeal, and are reproduced in the accompanying appendix. Claims 1, 2, 4, 5, 11-14 and 18 have been cancelled.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention claimed in claim 25 is directed to a client platform (100, 1001) adapted to provide restricted use of data provided by a server (1109), the client platform comprising a display (105, 1005); a secure communication means (310); a client trusted component (260, 1003) physically and logically protected from unauthorised modification to provide verification of the integrity of the platform to a user upon user request, the client trusted component having an associated memory (305) containing image receiving code (1004) for receiving data from a server by the secure communications means and for display of such data, and further having a display controller (320) (p. 9 l. 30 - p. 15 l. 28) such that the display is controlled from within the client trusted component; wherein the client platform is adapted such that the data received from the server is used for display of the data and not for an unauthorised purpose (p. 30 l. 7 - p. 34 l. 12, Figs. 1-3, 10).

The invention claimed in claim 26 is directed to a server (1109) adapted to provide data to a client platform (100, 1001) for restricted use by the client platform, comprising a memory containing image sending code (1103) for providing an image of data executed on the server; secure communications means (310) for secure communication of images to a client platform; and means to authenticate a trusted component (260, 1003) of a client platform, the trusted component having a display controller such that display of the data from the server is controlled from within the client trusted component (p. 30 l. 7 - p. 33 l. 8); whereby the server is adapted to

authenticate the trusted component of a client platform to determine that said client platform is adapted to ensure restricted use of the data before it is sent by the image sending code (p. 33 l. 10 - p. 34 l. 12, Figs. 1-3, 10).

The invention claimed in claim 28 is directed to a system for providing image data securely to a user for restricted use, comprising a client platform (100, 1001) comprising a display (105, 1005), a processor (200) adapted to allow secure communication with remote parties, a client trusted component (260, 1003) physically and logically protected from unauthorised modification to provide verification of the integrity of the platform to a user upon user request (p. 9 l. 30 - p. 15 l. 28), the client trusted component having an associated memory containing image receiving code (1004) for receiving data securely from a server (1109) and for display of such data and further having a display controller such that the display is controlled from within the client trusted component; and a server (1109) comprising a memory containing image sending code (1103) for providing an image of data executed on the server, a processor adapted to allow secure communication of images to the client platform and to authenticate a trusted component of the client platform; wherein the server is adapted to authenticate the trusted component of a client platform to determine that said client platform is adapted to ensure restricted use of the data before it is sent by the image sending code, the client platform is adapted such that the data received from the server is used for display of the data and not for an unauthorised purpose, and the system is adapted for a user on the client platform to request image data from the server to view at the client platform (p. 30 l. 7 - p. 34 l. 12, Figs. 1-3, 10).

The invention claimed in claim 29 is directed to a method of providing image data to a client platform (100, 1001) for restricted use, comprising a client platform requesting image data from a server (1109); the server determining that the client platform both has permission to receive image data, and has a client trusted component (260, 1003) physically and logically protected from unauthorised modification adapted to use the image data only for the restricted use and to control display of the image data from within the client trusted component; and provision of the image data over a secure communication channel (p. 30 l. 7 - p. 34 l. 12, Figs. 1-3, 10).

The invention claimed in claim 30 is directed to a client platform (100, 1001) adapted to provide restricted use of data provided by a server, the client platform comprising a display (105,

1005); a secure communication means (310); a user interface 105, 110, 115, 120); a client trusted component (260, 1003) physically and logically protected from unauthorised modification and able to lock the user interface (p. 9 l. 30 - p. 15 l. 28), the client trusted component having an associated memory containing image receiving code (1004) for receiving data from a server (1109) by the secure communications means and for display of such data and further having a display controller such that the display is controlled from within the client trusted component; wherein the client platform is adapted such that the data received from the server is used for display of the data and not for an unauthorised purpose (p. 30 l. 7 - p. 34 l. 12, Figs. 1-3, 10).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 26 and 29 are patentable under 35 U.S.C. 102(b) over WIPO Patent Publication No. 98/44402 to Bramhill et al. (hereinafter "Bramhill").

Issue 2: Whether claims 8 and 25 are patentable under 35 U.S.C. 103(a) over U.S. Patent No. 5,825,879 to Davis (hereinafter "Davis") in view of U.S. Patent No. 5,517,569 to Clark (hereinafter "Clark").

Issue 3: Whether claims 3, 6, 9, 15-17, 19-22, 25, 28 and 29 are patentable under 35 U.S.C. 103(a) over Bramhill and further in view of Davis and further in view of Clark.

Issue 4: Whether claims 10, 23 and 24 are patentable under 35 U.S.C. 103(a) over Bramhill and further in view of Davis and further in view of Clark and further in view of U.S. Pat. No. 5,990,927 to Hendricks (hereinafter "Hendricks").

Issue 5: Whether claims 7 and 27 are patentable under 35 U.S.C. 103(a) over Bramhill and further in view of Davis and further in view of Clark and further in view of U.S. Pat. No. 6,219,788 to Flavin (hereinafter "Flavin").

Issue 6: Whether claim 30 is patentable under 35 U.S.C. 103(a) over Bramhill and further in view of Davis and U.S. Pat. No. 5,355,414 to Hale et al. (hereinafter "Hale").

ARGUMENT

Issue 1: Whether claims 26 and 29 are patentable under 35 U.S.C. 102(b) over WIPO Patent Publication No. 98/44402 to Bramhill et al. (hereinafter "Bramhill").

In the final Office Action of November 26, 2007, the Examiner rejects claims 26 and 29 under 35 U.S.C. 102(b) as being anticipated by WIPO Patent Publication No. 98/44402 to Bramhill et al., once again asserting that:

> Bramhill discloses a server that securely sends data to an authenticated client. This inherently requires the server to have a memory from which an image of the program having this functionality can be executed. The authentication of the token may involve the use of a token sent to the client to verify that the client has permission and has not been tampered, ensuring that the client restricts use of the data (such as image data, which is displayed at a client) before it is sent.

In their previous submission, Appellants respectfully traversed because the above does not set forth a proper §102 rejection, explaining that the Examiner had failed to show that each and every claimed limitation is disclosed by Bramhill. Claim 26 recites, *inter alia*, means to authenticate a trusted component of a client platform, the trusted component having a display controller such that display of the data from the server is controlled from within the client trusted component. Appellants noted that there is nothing in Bramhill that can be understood as disclosing a trusted component of a client platform, nor disclosing or even alluding to a display controller such that display of data is controlled from within the client trusted component. Appellants once again explained that at most, Bramhill discloses that the client machine runs a Java-enabled browser that has the right-side mouse buttons disabled for a region displaying a particular image (i.e. the well known "save as", etc., commands). A Java-enabled browser is software and certainly does not read upon a trusted component (which is clearly disclosed to be hardware) having a display controller such that display of the data from the server is controlled from within the client trusted component.

Appellants further noted that Bramhill discloses that the authentication of the client may be done through a so-called dogtag program which is provided to the user through the mail to thereby ensure that the correct user receives is and thus provide "reasonable certainty" that the client machine running the dogtag program correspond to the correct user. Nevertheless, such a dogtag program also fails to anticipate the presently disclosed trusted component with display controller because (1) a program is not a component with a display controller, and (2) regardless,

there is no disclosure whatsoever that the dogtag program can control the display of information on the client machine.

Claim 26 further recites that the server is adapted to authenticate the trusted component of a client platform to determine that said client platform is adapted to ensure restricted use of the data before it is sent by the image sending code. The Examiner notes that the server of Bramhill does not provide data to a client unless the client is authenticated. However, there is nothing in Bramhill that teaches that authentication of a client determines that the client platform is adapted to ensure restricted use of the data. At page 11 Bramhill teaches that a client may be authenticated if it has made a payment, or if it known to the server in respect of some other service being provided and "the client's *credentials* may be authenticated by means of procedures already in use for the service." Neither of these types of authentication have any bearing upon determining that the client platform is adapted to ensure restricted use of the data - at best, they determine that the client platform has paid for use of the data. Similarly, the dogtag program exists solely "to provide a machine identification code (MID) which provides a substantially unique identification of the client." The dogtag program has no control whatsoever upon the display of data. Again, the only control over the display of the data is accomplished through the Java-enabled browser, and this browser does in no way anticipate a client trusted component having a display controller such that display of the data from the server is controlled from within the trusted component. Finally, Appellants noted that claim 26 recites means to *authenticate* such a trusted component, and there is nothing in Bramhill that discusses means on the server for authenticating the Java-enabled browser on a client.

Presently the Examiner retorts to the above by first invoking the "broadest reasonable interpretation in light of Applicant's specification" and then reiterating his earlier assertion "that though the client disclosed by Bramhill is not as well-protected as that of the instant application, it nonetheless constitutes a trusted component insofar as it is defined in the specification." Appellants have previously explained this is patently incorrect, as the specification clearly informed the reader that, *inter alia*:

> The trusted module or component is preferably immune to unauthorised modification or inspection of internal data. It is physical to prevent forgery, tamper-

> resistant to prevent counterfeiting, and preferably has cryptographic functions to securely communicate at a distance. Methods of building trusted modules are, per se, well known to those skilled in the art. The trusted module may use cryptographic methods to give itself a cryptographic identity and to provide authenticity, integrity, confidentiality, guard against replay attacks, make digital signatures, and use digital certificates as required…
>
> To achieve a trusted computing platform, there is incorporated into the computing platform a physical trusted device whose function is to bind the identity of the platform to reliably measured data that provides an integrity metric of the platform…
>
> The trusted device uses cryptographic processes but does not necessarily provide an external interface to those cryptographic processes. Also, a most desirable implementation would be to make the trusted device tamperproof, to protect secrets by making them inaccessible to other platform functions and provide an environment that is substantially immune to unauthorised modification. Since tamper-proofing is impossible, the best approximation is a trusted device that is tamper-resistant, or tamper-detecting. The trusted device, therefore, preferably consists of one physical component that is tamper-resistant…
>
> The trusted device is preferably a physical one because it must be difficult to forge. It is most preferably tamper-resistant because it must be hard to counterfeit. It typically has an engine capable of using cryptographic processes because it is required to prove identity, both locally and at a distance, and it contains at least one method of measuring some integrity metric of the platform with which it is associated.

Appellants respectfully invite the members of the Board to peruse the Bramhill reference in an attempt to identify *any* of the above features being taught by Bramhill in connection with his Internet browser running on a client computer, and submit for the Board's consideration that not one of these features is to be found in this reference. The Examiner's admission that the client disclosed by Bramhill "is not as well-protected" as that of the instant application severely

under-represents the chasm between claim 26 and the teachings of Bramhill. The teachings of Bramhill have absolutely no impact upon the client platform beyond the disabling of a few Internet browser functions by a downloaded applet, and the Examiner's assertion that this constitutes a trusted component insofar as the term is defined in the instant application's specification is simply untenable.

The specification as exemplified by the above excerpts also thoroughly disproves the Examiner's newly presented contention that "the client and program must be considered together and do anticipate Applicant's invention as claimed." This is doubly incorrect - there is nothing in the claim terms nor in the definitions of these terms set forth in the specification that supports the Examiner's contention that "the client and program *must* be considered together," and, again, even if considering the client and the program together, there is still no mention in Bramhill of any of the features of a trusted device as set forth in Appellant's specification.

Also for these very same reasons, the Examiner further present assertion that "Bramhill's disclosure clearly shows that the images being displayed are being controlled by software in the authenticated client" is irrelevant to claim 26, because as repeatedly explained above, Bramhill's "software in the authenticated client" does not read upon the presently claimed trusted component having a display controller.

With respect to claim 29, Appellant note that this claim similarly recites a server determining that the client platform both has permission to receive image data, and has a client trusted component physically and logically protected from unauthorized modification adapted to use the image data only for the restricted use and to control display of the image data from within the client trusted component. As explained above, there is no such client trusted component to be found in Bramhill, but rather only a Java-enabled browser that cannot be understood as being a "component physically and logically protected from unauthorised modification."

Applicants further disagree with the Examiner's assertion that "The authentication of the token may involve the use of a token sent to the client to verify that the client has permission and has not been tampered" because (1) there is no token mentioned in Bramhill, (2) there is nothing akin to a token mentioned in the claims, and (3) as explained above, there is no discussion whatsoever in Bramhill of checking whether a client has been *tampered* with - only whether the

client has paid a sum of money in order to be allowed to view a picture. The Examiner's present assertion that "Regarding Applicant's argument that Bramhill's invention does not check for tampering, that property is not explicitly claimed, and is not inherently necessary for a component to be 'trusted'," completely and conveniently ignores the other two points noted by Appellants - that there is not such thing as a token either recited in the claims nor mentioned in Bramhill. This assertion is therefore completely irrelevant to the present claims.

In view of the preceding, Appellants respectfully submit that the Examiner's interpretation of Bramhill is not supported by the plain language of the reference and clearly does not read upon the present claims, and thus requests that the Examiner be overturned on appeal with respect to claims 26 and 29.

Issue 2: Whether claims 8 and 25 are patentable under 35 U.S.C. 103(a) over U.S. Patent No. 5,825,879 to Davis (hereinafter "Davis") in view of U.S. Patent No. 5,517,569 to Clark (hereinafter "Clark").

In the final Action the Examiner once again rejects claims 8 and 25 under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Clark, and reiterates that with regard to claim 25, Davis discloses all of the claimed limitations with the exception of a mechanism for verifying the integrity of the platform upon user request, that Clark discloses a hardware test in a protected platform in which a user may initiate the verifying the platform's integrity, and that it would have been obvious to a skilled person to modify the invention of Davis by implementing it with a user-initiated integrity check as disclosed by Clark so that a user may have confidence in the platform that he or she is using.

Appellants have previously explained why this is not in fact reasonable or correct. Specifically, Appellants noted that the Examiner asserts that Davis discloses a trusted component logically protected from unauthorized modification at col. 3 ll. 27-43 and offers the explanation "protected key loading." The cited passage is reproduced below, and Appellant once again assert that this casts no light upon the Examiner's cryptic pronouncement of "protected key loading":

> In exchange for payment, or some other mutually agreed upon arrangement, the provider transfers a cryptographic key either to the SVCP directly through a

> connecting cable (e.g. telephone lines, cable, etc.) or to the user who subsequently loads the cryptographic key into the SVCP. The cryptographic key is needed for decoding the video to be viewed. The cryptographic key may be encrypted with the public key of the SVCP to ensure its security. Along with the needed cryptographic key, other authorization information may also be transferred. Such information may include, but is not limited to, the number of times a video may be watched or an expiration time upon which the video may no longer be watched. Thus, the encrypted video itself is useless without the cryptographic key, allowing the encrypted video to be provided by the provider or by other general distribution sources such as the internet.

This passage teaches that a cryptographic key must be loaded into the secure video content processor (the SVCP, which the Examiner asserts to read upon the presently claimed trusted component), and that this may be done directly through a cable or entered by a user through a keyboard. Appellants have explained that there is nothing in this passage to support the Examiner's interpretation of allegedly teaching that the SVCP is logically protected from unauthorized modification. The cryptographic key that is the subject of this passage is required for the SVCP to decrypt a particular video stream to be able to play it; the need for such a key certainly offers no logical protection against unauthorized *modification*, rather it offers protection of the video stream against unauthorized *display*.

Presently the Examiner answers by offering the further non sequitur "Davis' invention clearly includes protection against the use of unauthorized keys, including the encrypting of decryption keys, which one skilled in the art would recognize as *potentially frustrating* an attempt to misuse the system. It therefore enjoys *some protection* from unauthorized modification." [emphasis added] Appellants respectfully submit that these assertions have absolutely no bearing upon the novelty of claim 25, as the claim clearly does not recite *potentially frustrating* anyone nor offering *some protection* from unauthorized modification. Furthermore, the Examiner's assertion is simply incorrect - the keys are **not** provided for protecting the SVCP (the alleged trusted component), rather they are provided to prevent *unauthorized display* of a video file by the SVCP. There is absolutely no logical connection that can be drawn between the actual disclosure that teaches providing a key to the SVCP to enable it

to play a video file, and the Examiner's inference that upon providing such a key to the SVCP, the SVCP becomes somehow protected from unauthorized modification.

Appellants had previously also disagreed with the Examiner's rationale for combining the Davis and Clark references, who asserted that the skilled person would recognize that it is important for a user to have confidence in the platform that he or she is using. Appellants explained that the Davis reference is concerned with preventing unauthorized reproduction of a video distributed via the Internet, and solves the problem by providing a secure video content processor that is incorporated in the end-user's client platform (e.g. PC, set-top box, video game console) and forces the user to pay the video content provider before enabling the display of the video on the user's platform. Appellants thus submitted that the skilled person looking to implement this system would not be concerned with whether the user has confidence in his platform - after all, this platform is typically in the user's own bedroom or living room where there is no fear of unauthorized access to the platform. The entire raison d'être of Davis is to protect the video distributor, not the end user, and contemplating the addition of a platform verification option does nothing to further this purpose (protecting the distributor), and Appellants therefore disagree that there is any motivation for the skilled person to modify Davis' invention as asserted by the Examiner.

Furthermore, even if moved to implement the hardware testing feature of Clark into the system of Davis, there is simply no reason in the references or in common sense to implement it in the SVCP. "The SVCP is usually included within a video subsystem 116 implemented inside a PC 100, usually on a PCI bus compatible card much like a traditional graphics controller card." (col. 4 l. 21) Clark's hardware test operation 420 is one of quite a few software subroutines (menu options) within a remote transaction application program. Why would the skilled person lift one such subroutine out of this program and implement it within an ASIC on a graphics controller card? There is nothing in the references nor in the Examiner's discussion that would explain why the skilled person would take the much more complex and expensive route of implementing Clark's application program in the hardware of Davis, and Appellants thus submitted that the skilled person would at most provide the same application program to run on the user platform of Davis.

Presently the Examiner replies that "when there is a desire to make a system secure, it is reasonable for one skilled in the art to add additional layers of security to an invention. Though headend systems are typically installed in home environments, they can also be found in more secure locations. 'Users' in a deployment may just be the customers themselves (who themselves may have reasons for having an untampered system), but also technicians from the service provider." Appellants are completely befuddled by this assertion, as it does not address a single of Appellants' arguments, with the exception of the unsupported and incorrect assertion that headend systems "can also be found in more secure locations." Appellants submit to the Board that the Examiner has failed to make a proper showing of a reasonable, logical rationale for combining the Davis and Clark references, and his current "answer" is not only irrelevant but devoid of any substance.

Appellants submit that the Examiner's further contention that "Both of the references are to secure computing systems and are sufficiently analogous that one skilled in the art would find it advantageous to combine them" does not address the actual relevant 103 inquiry of whether one skilled in the art would be motivated to combine them; it is well settled that, with the full benefit of hindsight, most inventions would have been found advantageous by others.

Finally, Appellants note that they also disagreed with the Examiner's assertion that "by authenticating the received data, Davis' client in effect verifies the trusted status of another platform, the server" because Davis' client does not *authenticate* received data, it *decrypts* it. Decryption is not authentication, and the Examiner offered no explanation how authenticating data received from a server verifies the trusted status of that server - which Appellants submitted that in fact it cannot because authenticating received data simply verifies (that is, identifies) the source of the data, not a trusted status of that source. The Examiner presently retorts that "it is noted that since data from a bad source would fail the authentication check, a successful authentication affirms that a source is, at least to some extent, trustworthy." This is again predicated on the incorrect reading of Davis that the Examiner insists on, because in fact there is no **authentication** check in Davis. Davis teaches decryption of received data. Decryption of received data does not authenticate the source of that data, regardless of the Examiner's insistence to the contrary.

Appellants thus respectfully submit that the Examiner's 103 rejection of claim 25 is not supported by the cited references nor by logic, and request the Board to kindly consider the above and overturn the Examiner on appeal. Appellants further note that claim 8 is dependent on claim 25, and thus this claim is novel and patentable over the art on record at least in view of its dependency on claim 25.

Appellants further respectfully submit that the Examiner's rejection falls short of the requirements for a proper 35 USC §103 rejection as set forth in the MPEP as well as the new *KSR v. Teleflex* Examination Guidelines of October 10, 2007.

The new Guidelines provide that "When making an obviousness rejection, Office personnel must therefore ensure that the written record includes findings of fact concerning the state of the art and the teachings of the references applied. In certain circumstances, it may also be important to include explicit findings as to how a person of ordinary skill would have understood prior art teachings, or what a person of ordinary skill would have known or could have done. Factual findings made by Office personnel are the necessary underpinnings to establish obviousness." There is an utter dearth of such *factual* findings in the present Action, and in their stead conclusory statements as to what the skilled person, according to the Examiner's unsupported and unexplained opinion, would allegedly have done.

The Guidelines further admonish that "Although a rejection need not be based on a teaching or suggestion to combine, a preferred search will be directed to finding references that provide such a teaching or suggestion if they exist." The Examiner has not even acknowledged this pronouncement, much less provided a reason for the complete lack of such teaching or suggestion in any of the cited references.

The Guidelines further set forth that "Any obviousness rejection should include, either explicitly or implicitly in view of the prior art applied, an indication of the level of ordinary skill." No such indication, explicit or implicit, is to be found in the Examiner's Action.

Perhaps the most instructive portion of the Guidelines is the clear statement that "The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Court quoting *In re*

Kahn stated that " '[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.' " Again, rather than offer articulated reasoning with some rational underpinning, the Examiner merely asserts a conclusion of obviousness.

These Guidelines do make clear that "the familiar teaching-suggestion-motivation (TSM) rationale" can still be employed by Examiners in making an obviousness rejection. However, as noted above, the Examiner has not even mentioned where such suggestion is allegedly to be found in any of the cited references.

Issue 3: Whether claims 3, 6, 9, 15-17, 19-22, 25, 28 and 29 are patentable under 35 U.S.C. 103(a) over Bramhill and further in view of Davis and further in view of Clark.

The Examiner further rejects claims 3, 6, 9, 15-17, 19-22, 25, 28 and 29 under 35 U.S.C. 103(a) as being unpatentable over Bramhill as applied to claim 26 and further in view of Davis and further in view of Clark. Appellants note the previous discussion of Bramhill and Davis, wherein it is explained that these references each omits at least one claimed element contrary to the Examiner's assertion, and thus submit that the above discussion is equally probative of the non-obviousness and patentability of these claims over the combination of Bramhill, Davis and Clark. Specifically, Davis does not in fact disclose a trusted component with display controller as claimed, and even if applying Davis' tamper-proofing at the client to Bramhill, the skilled person would still not obtain a client trusted component physically and logically protected from unauthorized modification to provide verification of the integrity of the platform to a user upon user request and further having a display controller such that the display is controlled from within the client trusted component.

Furthermore, the Examiner's proffered motivation to combine the two references does not make complete sense - why would the skilled person add the significant expense and complexity of tamper-proofing the client hardware as per Davis when Bramhill already "makes it more difficult to capture the unencrypted digital representation" by disabling select software functions in the client platform? Although Davis and Bramhill are concerned with the same

problem (preventing unauthorized distribution of digital content), they provide completely different solutions - Bramhill downloads an applet together with the content that controls the user's platform to the extend the content is displayed, whereas Davis provides specific hardware on the user's platform. These are completely opposite approaches to the same problem, and combining them is no easy feat nor advantageous from an engineering point of view - and the Examiner has once again not made a showing of why the skilled person would have a reasonable expectation of success when attempting to combine these two radically different solutions. Appellants thus submitted that the motivation asserted by the Examiner to combine these two references, "to make it more difficult to capture the unencrypted digital representation," simply does not exist outside of the Examiner's hindsight because making it more difficult to capture the unencrypted digital representation is the very purpose of Bramhill and the skilled person has no reason to look to another reference for another solution to the same exact problem.

Presently the Examiner answers by asserting that "Bramhill does not give specifics as to what kind of display should be used. Davis and Clark's invention is a display controller, and can therefore easily be combined into Bramhill to fulfill that role. Since each invention contributes attributes that make the whole system more secure, it would be obvious to combine them all in order to enjoy greater overall security." Appellants submit that this fails to offer an actual *proof* for the Examiner's position, as his assertion that the display controller can *easily* be combined into Bramhill enjoys not one bit of support in the Examiner's answer, the references themselves, or any other knowledge in the art identified by the Examiner.

Appellants thus respectfully submit that claims 3, 6, 9, 15-17, 19-22, 25, 28 and 29 are in fact non-obvious and patentable over the art on record and request the Board to kindly overturn the Examiner on appeal.

Issue 4: **Whether claims 10, 23 and 24 are patentable under 35 U.S.C. 103(a) over Bramhill and further in view of Davis and further in view of Clark and further in view of U.S. Pat. No. 5,990,927 to Hendricks (hereinafter "Hendricks").**

The Examiner rejects claims 10, 23 and 24 under 35 U.S.C. 103(a) as being unpatentable over Bramhill as applied to claims 26 and 29 and further in view of Davis and Clark and further in view of Hendricks. Appellants note the above discussion of Bramhill, Davis, and Clark and submit that this discussion is equally probative of the non-obviousness and patentability of claims 10, 23 and 24 at least because these claims depend from claims that have been shown above to be novel and non-obvious over the art on record. Appellants thus respectfully request the Board to overturn this rejection on appeal.

Issue 5: Whether claims 7 and 27 are patentable under 35 U.S.C. 103(a) over Bramhill and further in view of Davis and further in view of Clark and further in view of U.S. Pat. No. 6,219,788 to Flavin (hereinafter "Flavin").

The Examiner rejects claims 7 and 27 under 35 U.S.C. 103(a) as being unpatentable over Bramhill as applied to claims 26 and 29 and further in view of Davis and Clark and further in view of Flavin. Appellants note the above discussion of Bramhill, Davis, and Clark and submit that this discussion is equally probative of the non-obviousness and patentability of claims 7 and 27 at least because these claims depend from claims that have been shown above to be novel and non-obvious over the art on record. Appellants thus respectfully request the Board to overturn this rejection on appeal.

Issue 6: Whether claim 30 is patentable under 35 U.S.C. 103(a) over Bramhill and further in view of Davis and U.S. Pat. No. 5,355,414 to Hale et al. (hereinafter "Hale").

The Examiner rejects claim 30 under 35 U.S.C. 103(a) as being unpatentable over Bramhill as applied to claim 26 and further in view of Davis and Hale. Appellants once again submit that the combination of Bramhill and Davis is not in fact obvious to the skilled person, as shown above. Furthermore, Hale does not in fact teach locking a user interface, contrary to the Examiner's assertion:

> In one embodiment, the host computer is in communication with a display, and the peripheral device controller is further responsive to the predetermined period during which the peripheral input device remains inactive to send signals to

> the host to deactivate the display so that information visible on the display is not viewable. In this embodiment, the peripheral input device is further responsive to the predesignated signals from the peripheral input device to restore operation of the display. [col. 3, ll. 27-33, cited by the Examiner]

The above teaches deactivating a display - how can this possibly be understood as locking a user interface? A user interface consists of a display and at least an input device (keyboard, mouse, etc.). Locking such an interface clearly means preventing the user from interfacing with the platform including preventing input by the user. Where is any of this even alluded to in Hale?

Furthermore, why would the skilled person implementing Bramhill's or Davis' systems care to prevent the display of insecure information? Where could such "insecure information" possibly come from in Bramhill or Davis? What possible benefit could be added to either Bramhill or Davis, which are specifically concerned with very strictly controlling the display of certain data, by endowing it with the ability to lock the interface to the user's platform? For that matter, what user would care to download data from a server using either Bramhill or Davis' invention if the user interface on his platform could be locked by the server? Adding this feature to either Bramhill or Davis simply makes no sense.

The Examiner presently answers the above by reasoning that "since the user interface is dependent upon the display, the loss of the display renders the user interface useless, thus effectively locking it. Since Hale's modification provides further protection from misuse over and above that provided in the other references, one skilled in the art would reasonably be motivated to incorporate it in order to further enhance security." Appellants respectfully disagree that "the user interface is dependent upon the display" and that "the loss of the display renders the user interface useless, thus effectively locking it" because as anyone who has ever used a computer could inform the Examiner, the user interface consists typically of the display and input devices such as a keyboard and mouse, and one can most certainly enter commands via the keyboard regardless of whether the display has been disabled or not - the Examiner appears to assert that one must see what one is typing in order to do so, and Appellants submit that the fallacy of this assertion is self evident.

Appellants thus respectfully submit that claim 30 is also non-obvious and patentable over the art on record and request the Board to kindly overturn the Examiner on appeal.

* * *

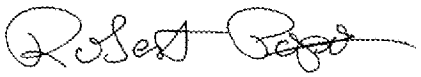
CONCLUSION

For the many reasons advanced above, Appellants respectfully contend that each pending claim is patentable and reversal of all rejections and allowance of the case is respectfully solicited.

I hereby certify that this document is being transmitted to the Patent and Trademark Office via electronic filing.

April 25, 2008
(Date of Transmission)

Respectfully submitted,



Robert Popa
Attorney for Appellants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@la.ladas.com

CLAIMS APPENDIX

3. A client platform as claimed in claim 25, wherein the client trusted component contains an integrity monitor adapted to provide a measure of the integrity of code operating on the client platform, and the integrity monitor is adapted to monitor the integrity of the image receiving code.

6. A client platform as claimed in claim 25, wherein the client platform further comprises a secure user interface for providing user input directly to the client trusted component, and wherein the image receiving code is adapted to provide user input received from the secure user interface to a server.

7. A client platform as claimed in claim 25, wherein the client trusted component is adapted to authenticate other trusted components or secure tokens.

8. A client platform as claimed in claim 25, wherein the client trusted component is adapted to determine a trusted status of other platforms.

9. A client platform as claimed in claim 25, also comprising a smart card reader for receiving a Smart card comprising a user's secure token.

10. A client platform as claimed in claim 25, wherein a part of the display is reserved for display of data determined by the server independent of any request by the client platform.

15. A system as claimed in claim 28, adapted for a user to request execution of code on the client platform to provide image data to be viewed at the client platform.

16. A system as claimed in claim 25, adapted for a user to request execution of

code, and for code then to be executed partly on the client platform and partly on the server to provide image data to be viewed at the client platform, wherein the image data is viewed at the client platform in association with the results of code executed on the client platform.

17. A system as claimed in claim 28, wherein the client platform comprises a smart card reader for receiving a smart card comprising a user's secure token, further comprising a user smart card wherein the server is adapted to determine that the user smart card is such as to allow the image data to be sent to the client platform.

19. A method as claimed in claim 29, further comprising provision of request data from the client platform to the server, and provision of modified image data based on the request data.

20. A method as claimed in claim 19, wherein the provision of request data and the provision of modified image data are repeated as often as required.

21. A method as claimed in claim 29, further comprising updating of a usage log after image data or modified image data is provided to the client platform.

22. A method as claimed in claim 29, wherein the step of determining permission comprises determining whether a smart card containing a user permission is in session with the client platform.

23. A method as claimed in claim 29, wherein a part of the image data is determined by the server independent of any request from the client platform.

24. A method as claimed in claim 23, wherein said part of the imaging data comprises advertising content.

25. A client platform adapted to provide restricted use of data provided by a server,

the client platform comprising:

a display;

a secure communication means;

a client trusted component physically and logically protected from unauthorised modification to provide verification of the integrity of the platform to a user upon user request, the client trusted component having an associated memory containing image receiving code for receiving data from a server by the secure communications means and for display of such data, and further having a display controller such that the display is controlled from within the client trusted component;

wherein the client platform is adapted such that the data received from the server is used for display of the data and not for an unauthorised purpose.

26. A server adapted to provide data to a client platform for restricted use by the client platform, comprising:

a memory containing image sending code for providing an image of data executed on the server;

secure communications means for secure communication of images to a client platform; and

means to authenticate a trusted component of a client platform, the trusted component having a display controller such that display of the data from the server is controlled from within the client trusted component;

whereby the server is adapted to authenticate the trusted component of a client platform to determine that said client platform is adapted to ensure restricted use of the data before it is sent by the image sending code.

27. A server as claimed in claim 26, containing a server trusted component physically and logically protected from modification, wherein said server trusted component contains the means to authenticate a trusted component.

28. A system for providing image data securely to a user for restricted use, comprising:

a client platform comprising a display, a processor adapted to allow secure communication with remote parties, a client trusted component physically and logically protected from unauthorised modification to provide verification of the integrity of the platform to a user upon user request, the client trusted component having an associated memory containing image receiving code for receiving data securely from a server and for display of such data and further having a display controller such that the display is controlled from within the client trusted component; and

a server comprising a memory containing image sending code for providing an image of data executed on the server, a processor adapted to allow secure communication of images to the client platform and to authenticate a trusted component of the client platform;

wherein the server is adapted to authenticate the trusted component of a client platform to determine that said client platform is adapted to ensure restricted use of the data before it is sent by the image sending code, the client platform is adapted such that the data received from the server is used for display of the data and not for an unauthorised purpose, and the system is adapted for a user on the client platform to request image data from the server to view at the client platform.

29. A method of providing image data to a client platform for restricted use, comprising:

a client platform requesting image data from a server;

the server determining that the client platform both has permission to receive image data, and has a client trusted component physically and logically protected from unauthorised modification adapted to use the image data only for the restricted use and to control display of the image data from within the client trusted component; and

provision of the image data over a secure communication channel.

30. A client platform adapted to provide restricted use of data provided by a server, the client platform comprising:

a display;

a secure communication means;

a user interface;

a client trusted component physically and logically protected from unauthorised modification and able to lock the user interface, the client trusted component having an associated memory containing image receiving code for receiving data from a server by the secure communications means and for display of such data and further having a display controller such that the display is controlled from within the client trusted component;

wherein the client platform is adapted such that the data received from the server is used for display of the data and not for an unauthorised purpose.

EVIDENCE APPENDIX

There is no evidence submitted with the present Brief on Appeal.

RELATED PROCEEDINGS APPENDIX

There are no other appeals or interferences related to the present application.